一种移动 P2P 网络环境下的动态安全信任模型

李致远[1,2],王汝传[1,3,4]

(1.南京邮电大学计算机学院,江苏南京 210003; 2.江苏大学计算机科学与通信工程学院,江苏镇江 212013;
3.江苏省无线传感网高技术研究重点实验室,江苏南京 210003; 4.南京邮电大学计算机研究所,江苏南京 210003)

摘 要: 信任是移动对等(MP2P)网络安全中首要解决的关键技术问题.由于 MP2P 网络环境与 P2P 网络环境有本质的区别,因此现有 P2P 网络信任模型并不适用于 MP2P 网络环境.本文提出一种适合 MP2P 网络环境的动态安全信任模型 DSTM_MP2P.DSTM_MP2P 包括两种方案,一种是针对节点的信任信息已知或部分已知的情况,提出基于节点行为的节点类型识别机制;另一种是针对节点的信任信息未知的情况,提出基于贝叶斯博弈的节点概率选择策略.通过理论分析和实验证明,无论 MP2P 网络环境如何,DSTM_MP2P 模型使得请求节点总是优先连接安全可靠的节点,从而极大地提高了下载成功率.

关键词: 移动对等网络; 安全; 信任; 博弈; 节点行为

中图分类号: TP393 **文献标识码:** A **文章编号:** 0372-2112 (2012) 01-0001-07

电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2012.01.001

A Dynamic Secure Trust Model for Mobile P2P Networks

LI Zhi-yuan[1,2], WANG Ru-chuan[1,3,4]

(1. *College of Computer, Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu* 210003, *China*;
2. *School of Computer Science and Telecommunication Engineering, Jiangsu University, Zhenjiang, Jiangsu* 212013, *China*;
3. *High Technology Research Key Lab of Wireless Sensor Networks, Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu* 210003, *China*;
4. *Institute of Computer, Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu* 210003, *China*)

Abstract: Trust is the most important key issue for Mobile P2P(MP2P) networks security. As the MP2P networks and the P2P networks environments are fundamentally different, the existing trust models for P2P networks are not suitable for MP2P networks. In view of this, a dynamic secure trust model for MP2P networks (DSTM_MP2P) is proposed. DSTM_MP2P is comprised of two schemes. One is node type-identifying mechanism based on node behavior under the situation of the known or part of the known trust information of the nodes. And the other is node probability selection strategy based on Bayesian game under the situation of the unknown trust information of the nodes. The theoretical analysis and experimental results show that whatever MP2P network environment is, a request node under the direction of the DSTM_MP2P model is always first to connect the safe and reliable nodes, which greatly increases the downloading success rate.

Key words: mobile peer to peer networks; security; trust; game theory; node behavior

1 引言

移动对等网络(Mobile Peer-to-Peer Networks,简称 MP2P)正受到了工业界和学术界的双重关注,逐渐成为一个新的研究热点.但由于 MP2P 网络中节点移动性和高度自治性,使得 MP2P 网络成为一个比 P2P 网络更加难以管理的网络环境.在这样的环境下,MP2P 网络安全就成为一个不可忽视的问题.而信任是 MP2P 网络安全中首要解决的关键技术问题.考虑到 MP2P 网络中节点资源的有限性以及稀缺的无线网络资源,现有的 P2P 网络信任方案及研究思路并不适合 MP2P 环境.因此,有必要对 MP2P 网络中信任问题进行深入地研究.目前提

收稿日期:2010-08-23;修回日期:2011-01-20

基金项目:国家自然科学基金(No.60973139, No.60773041, No.61003039, No.61003236);江苏省科技支撑计划(工业)项目(No.BE2010197, No.BE2010198);江苏省级现代服务业发展专项资金;江苏省高校自然科学基础研究项目(No.10KJB520013);高校科研成果产业化推进工程项目(No.JH10-14);国家和江苏省博士后基金(No.20090451240, No.20090451241, No.20100471353, No.20100471355);江苏高校科技创新计划项目(No.CX10B-196Z, No.CX10B-197Z, No.CX10B-198Z, No.CX10B-199Z, No.CX10B-200Z);江苏省六大高峰人才项目(No.2008118);江苏省计算机信息处理技术重点实验室基金(2010)

出的 P2P 网络信任模型都是建立在请求节点交互前总可以在有限跳内获得其他节点的信誉值的条件下,但 MP2P 网络与 P2P 网络的环境差别很大,在 MP2P 网络中,常会出现 Peer 节点无法获取到其邻居信誉值的情形,这使得节点间无法建立有效的信任关系,并导致 P2P 系统处于混乱状态甚至崩溃.其次,现有的 P2P 网络信任模型计算复杂度高且信誉值更新的通信代价大.这些都是无线网络及移动终端所无法承受的.

鉴于此,本文提出一种适合 MP2P 网络环境的动态安全信任模型 DSTM_MP2P(Dynamic Secure Trust Model for MP2P Networks).DSTM_MP2P 考虑到 MP2P 网络环境下资源请求节点对资源节点的历史行为信息可能是已知、部分已知或者未知 3 种情况,DSTM_MP2P 采用两种不同解决方案.首先针对资源节点的历史行为信息可能是已知、部分已知的情况,DSTM_MP2P 采用基于节点行为函数的节点类型识别机制.然后,针对资源节点的历史行为信息未知的情况,DSTM_MP2P 采用基于贝叶斯博弈的节点概率选择策略.最后,通过理论分析和实验证明 DSTM_MP2P 模型使得请求资源节点总是优先连接安全可靠的节点,从而大大提高了文件下载成功率.

2 相关工作

当前国内外对 P2P 网络信任模型进行了大量的研究,而对于 MP2P 环境下的信任问题的研究相对较少.下面首先对国内外的 P2P 网络信任模型研究成果进行总结,然后对 MP2P 环境下的信任解决方案进行介绍.

(1)P2P 网络信任模型

文献[1]提出了基于相似度加权推荐的信任模型 SWRTrust.该模型以节点评分行为的相似度加权其推荐度计算全局信任值.文献[2]提出基于声誉的信任模型 PeerTrust.该模型对实体得到的评价反馈进行统计和分类计算得到实体的信任值,并在此基础上建立信任关系.文献[3]提出基于改进 D-S 证据的信任模型,模型解决了汇聚推荐信息时无法处理不确定性及强行组合矛盾推荐信息引起的性能下降问题.文献[4]提出一种基于集对分析的信任模型.文献[5]提出了一种 P2P 网络环境下基于 Gossip 的信任值快速融合模型,并采用 Bloom 滤波器对节点的信任值进行分类存储及快速检索.文献[6]提出一种基于角色信任链的启发式发现算法,该算法鼓励 P2P 网络中的节点与善意节点共享资源,并排斥与恶意或者自私节点进行资源共享.文献[7]提出一种整合历史和当前节点性能数据的 P2P 信任模型.从上述研究成果发现,对信任模型中 Peer 间的信任关系刻画的技术路线是从随机性到模糊性,再到不确定性.随着对信任关系刻画的准确度越来越高,其相应的计算和存储复杂度也大幅上升.这些代价对有线网络影响不大,但对于无线网络却是无法承受的.因此,现有的 P2P 网络信任模型不能直接移植到 MP2P 网络环境下.

(2)MP2P 网络下的信任机制研究

文献[8]提出一种可信的移动环境框架的概念.该框架以信任理论为核心理念层、信任模型和标准为理论可操作层并以移动应用系统作为应用层.文献[9]提出 MP2P 环境下请求节点碰到陌生节点,即对陌生节点的历史行为不可知的情况下,是否与其进行交互的问题.然后首次提出使用信任来解决该问题,并给出 MP2P 信任解决方案应具有以下特点:①信任方案是分布式、轻量级的;②对陌生节点应采用随机策略;③拓扑模型应采用双层架构.文献[10]在 MP2P 项目——iClouds 的基础上,提出了基于信任的信息交互机制以保障 MP2P 安全.

3 MP2P 网络动态安全信任模型

3.1 DSTM_MP2P 模型的相关定义

DSTM_MP2P 模型常用的符号定义如表 1 所示.

表 1 符号定义

符号	描述
a_{ij}^t	节点 i 对节点 j 在 t 时刻的信任评价
$X_i(t)$	节点 i 在 t 时刻的全局信誉值
$f_i(t)$	节点 i 随时间变化的行为函数曲线
$chunk(\tau)$	第 τ 个文件分块
$\boldsymbol{TrustMatrix}(t)$	t 时刻 MP2P 网络中节点间的信任评价矩阵
$\boldsymbol{TrustMatrix}_i^t$	在第 i 个超级节点上存放的 t 时刻信任评价矩阵
q_{ij}^t	t 时刻,节点 i 从节点 j 下载成功的文件块数
N_{req}	请求资源节点集合
$N_{resources}$	资源节点集合
$\{SP_o, 1\leqslant o\leqslant k\}$	超级节点集合
$\{MP_e, 0\leqslant e\leqslant m\}$	普通节点集合

定义 1(节点间信任评价矩阵的全局视图) MP2P 网络中所有节点通过交互获得的信任评价矩阵如式(1)所示,它是由物理存储在 $\{SP_o, 1\leqslant o\leqslant k\}$ 上的局部信任评价矩阵求并得到的.

$$\boldsymbol{TrustMatrix}(t)=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mm} \end{pmatrix}_{m\times m} \tag{1}$$

定义 2(位图,bitmap) 在 $\{MP_e, 0\leqslant e\leqslant m\}$ 集合中的所有节点的缓冲区中建立 bitmap 数据结构,它的作用是记录和统计从资源节点下载文件块成功或失败的概率.

定义 3(网络中节点的类型及其特征) 假设网络中共有 3 类节点,分别是善意节点、恶意节点和伪善节点.善意节点的行为特征曲线是单调增,恶意节点的行

为特征曲线是单调减,而伪善节点的行为特征曲线是振荡的.

3.2 动态安全信任模型 DSTM_MP2P

3.2.1 基于节点行为的节点类型识别机制

针对资源节点的历史行为信息可能是已知、部分已知的情况,首先根据已知的信任评价值构建全局信任评价矩阵,然后在此基础上对矩阵的列向量单独处理并拟合生成节点的行为函数,最后通过对行为函数性质的研究达到辨识节点类型的目标.

(1)信任矩阵的生成和更新算法描述如下:

设请求资源节点集合为 $N_{req}\{mp_1, mp_2, \cdots, mp_n\}$,资源节点集合为 $N_{resources}\{r_1, r_2, \cdots, r_n\}$.

①对于 $\forall\ mp_i, i\in[1,n]$来说,$N_{resources}\{r_1, r_2, \cdots, r_n\}$向 mp_i 提供的文件分块如式(2)所示.

$$\begin{aligned} r_1 &\rightarrow mp_i \Leftrightarrow \bigcup_{\tau=1}^{w} chunk(\tau) \\ &\vdots \\ r_{n-1} &\rightarrow mp_i \Leftrightarrow \bigcup_{\tau=(n-1)w}^{nw} chunk(\tau) \\ r_n &\rightarrow mp_i \Leftrightarrow \bigcup_{\tau=nw}^{(n+1)w} chunk(\tau) \end{aligned} \tag{2}$$

②当 mp_i 从 $N_{resources}\{r_1, r_2, \cdots, r_n\}$下载文件分块后,会对下载文件块进行校验.

③mp_i 对步骤②得到的 bitmap 进行统计,得到 $q_{ij}^t, j\in[1,n]$.

④mp_i 将 $q_{ij}^t, j\in[1,n]$发送到 $SP_o, 1\leqslant o\leqslant k$.

⑤SP_o 根据式(3)得到 $a_{ij}^t, j\in[1,n]$,其中 w 为文件块的大小.

$$a_{ij}^t = \frac{q_{ij}}{w}, j\in[1,n] \tag{3}$$

⑥通过定义 1,$SP_o, 1\leqslant o\leqslant k$ 得到信任评价矩阵的全局视图 ***TrustMatrix***(t).

⑦对于第 $t+1$ 时刻,$a_{ij}^{t+1} = a_{ij}^t + a_{ij}^{t+1}, j\in[1,n]$,那么对于第 $t+h$ 时刻,$a_{ij}^{t+h} = \sum_{h=0}^{h} a_{ij}^{t+h}, j\in[1,n]$.

(2)节点行为函数的构造

获得 t 时刻的全局信任评价矩阵 ***TrustMatrix***(t)后,对其列向量求和,得到网络中所有节点对节点 j 在 t 时刻的信任评价值.

$$a_{ij}^t = \sum_{i=1}^{m} a_{ij}^t, j\in[1,m] \tag{4}$$

依此类推,可得到网络中所有节点对节点 j 在 $t+h$ 时刻的信任评价值.

$$a_{ij}^{t+h} = \sum_{i=1}^{m} a_{ij}^{t+h}, j\in[1,m], h\in[0,+\infty] \tag{5}$$

对 $a_{ij}^t, a_{ij}^{t+1}, a_{ij}^{t+2}, \cdots, a_{ij}^{t+h}$可用矩阵形式简记为

$$y = \boldsymbol{X}\boldsymbol{p}^{\mathrm{T}} + \varepsilon \tag{6}$$

其中 y 表示节点间的信任评价值,$\boldsymbol{p}$ 表示多项式系数,ε 表示白噪声,$\boldsymbol{X}$ 是关于时间的多项式矩阵.在 $SP_o(0<o<k)$上,利用最小二乘拟合求得节点的行为变化函数 $f_j(t)$.下面采用研究信任评价函数 $f_j(t)$的性质的方法达到区分节点类型的目标.

(3)基于节点行为函数的节点类型识别方法

定理 1(节点类型的识别定理)　在 $t\in(0,+\infty)$内,如果 $f_j(t)$的驻点唯一,不妨设为 t_0,那么当且仅当 $f_j'(t)>0$时,节点为善意节点;当且仅当 $f_j'(t)<0$时,节点为恶意节点;设在 $t\in(0,t_0]$内的导数为 $f_j'(t_-)$,在 $t\in(t_0,+\infty)$内的导数为 $f_j'(t_+)$,那么当 $f_j'(t_-)\cdot f_j'(t_+)<0$时,节点为伪善节点.如果 $f_j(t)$的驻点不唯一,那么节点一定为伪善节点.

证明　在 $t\in(0,+\infty)$内,令 $f_j'(t)=0$,得到驻点的集合$\{t_i, i\in\mathbb{Z}^+\}$.当驻点集合中的元素仅有一个,即驻点唯一时,对 $f_j(t)$求一阶导.若恒有 $f_j'(t)>0$,则 $f_j(t)$在定义域内是单调增函数,这就表明节点 j 为善意节点;若恒有 $f_j'(t)<0$,则 $f_j(t)$在定义域内是单调减函数,这就表明节点 j 为恶意节点;若 $t\in(0,t_0]$上的导函数 $f_j'(t_-)$和 $t\in(t_0,+\infty)$上的导函数 $f_j'(t_+)$乘积为负数,即有 $f_j'(t_-)\cdot f_j'(t_+)<0$.此时,网络中的节点对节点 j 的信任评价随时间 t 呈现出增减或减增的振荡变化,这就表明节点 j 一定为伪善节点.当驻点集合中的元素个数大于 1,即驻点不唯一时,显然网络中其他节点对节点 j 的信任评价随时间 t 呈现出增减或减增的周期性振荡变化,此时节点一定为伪善节点.

定理 2(伪善节点的周期振荡性)　在 $f_j(t)$的定义域 t 上,假设存在时间点序列 $t_0, t_1, t_2, \cdots, t_i, t_{i+1}, \cdots$,$\Delta t_0, \Delta t_1, \cdots, \Delta t_i$ 为时间点序列的差.如果 $\Delta t_0, \Delta t_1, \cdots, \Delta t_i$近似相等,且在区间$\Delta t_0, \Delta t_1, \cdots, \Delta t_i$上恒有$f_j'(t)>0$(或 $f_j'(t)<0$),$f_j''(t)>0$(或 $f_j''(t)<0$).则 $f_j(t)$在定义域 t 上是近似周期性振荡的.

证明　设函数 $f_j(t)$的驻点为 $t_0, t_1, t_2, \cdots, t_i, t_{i+1}, \cdots$,利用差分的思想,有 $\Delta t_0 = t_1 - t_0, \cdots, \Delta t_i = t_{i+1} - t_i, \cdots$.如果 $\Delta t_0 \approx \Delta t_1 \approx \cdots \approx \Delta t_i$,对 Δt_i 子区间内的 $f_j(t)$求一阶导和二阶导.若恒有 $f_j'(t)>0$(或 $f_j'(t)<0$),$f_j''(t)>0$(或 $f_j''(t)<0$),那么函数 $f_j(t)$是近似以周期 Δt_i 周期性振荡的.如果不满足 $\Delta t_0 \approx \Delta t_1 \approx \cdots \approx \Delta t_i$ 的条件,那么进一步进行差分,有 $\Delta t_0 = t_2 - t_0, \cdots, \Delta t_i = t_{2(i+1)} - t_{2i}, \cdots$.如果此时满足 $\Delta t_0 \approx \Delta t_1 \approx \cdots \approx \Delta t_i$ 条件,则和上述步骤证明相同.如果仍不满足条件,则进一步做差分,在 $n, n\rightarrow\infty$ 步之后,若始终不满足区间近似相等的条件,则表明 $f_j(t)$是不满足周期性振荡的.

对于满足定理 2 的伪善节点行为函数,通过该定理

可以找到伪善节点 j 的行为规律.这样便于最大化地利用伪善节点的善意时段向系统提供资源,遏制伪善节点在恶意时段向系统提供虚假或病毒资源.

3.2.2 基于贝叶斯博弈的节点概率选择策略

针对资源节点的历史信息未知的情况,往往出现在动态临时场景中,比如在车站候车,这些节点彼此间相互陌生,且在同一场景下的时间有限.当节点彼此分开之后,再次相遇的概率是小概率事件.在此网络环境下,仅存在善意和恶意两类节点.下面就对该问题利用博弈的方法进行研究.

定义 4 贝叶斯静态博弈简记为 $G=[N,\{T_i\},P,\{S_i(t_i)\},\{u_i\}]$.

①局中人集合 $N=\{1,2\}$.

②每个局中人都有一个类型空间 $T_i=\{t_i\},i\in N$.在全体类型空间 $T=\prod_{i=1}^{n}T_i$ 上的概率分布 $P(t_1,t_2,\cdots,t_n)$.

③每个局中人有(与自身的类型 t_i 相关的)策略集 $S_i=\{s_i\},i\in N$.且策略集 S_i 与其他局中人类型无关.

④每一个局中人都有其收益函数 $u_i(s_1,s_2,\cdots,s_n,t_i)$.

以上 4 个因素是共识的,局中人在以上情况下同时选择策略以追求自身的利益最大化.下面对 mp_i 与 r_i 的博弈进行描述.

节点 mp_i 要从它获取到的资源列表中提取出安全可靠的节点.资源列表中的节点 r_i 可能是善意节点,也可能是恶意节点.但节点 mp_i 不知道节点 r_i 属于哪一种类型,仅 r_i 自己知道自身属于哪种类型.该博弈规范式见表 2.

表 2 mp_i 与 r_i 博弈规范式

			mp_i	
			建立连接	不建立连接
r_i	善意节点	为 RP_i 提供可靠资源	(1,1)	(0,-2)
		不为 RP_i 提供资源	(0,-1)	(0,0)
	恶意节点	为 RP_i 提供虚假资源	(1,-2)	(-1,1)
		为 RP_i 提供携带病毒的资源	(2,-4)	(-2,2)

根据海萨尼转换策略,由自然决定了 r_i 有两种类型,$T_1=\{t_{11},t_{12}\}$,其中 t_{11}代表善意节点,t_{12}代表恶意节点.而 mp_i 仅有一种类型,$T_2=\{t_2\}$.

当 r_i 为善意节点时,其策略集 $S_1(t_{11})=\{s_1^{(1)}(t_{11}),s_2^{(1)}(t_{11})\}$,$s_1^{(1)}(t_{11})$代表为 mp_i 提供安全可靠的资源,$s_2^{(1)}(t_{11})$代表不为 mp_i 提供资源.r_i 此时采用$s_1^{(1)}(t_{11})$策略的概率为 x_1,采用 $s_2^{(1)}(t_{11})$策略的概率为 $1-x_1$,$x_1\in[0,1]$.当 r_i 为恶意节点时,其策略集 $S_1(t_{12})=\{s_1^{(1)}(t_{12}),s_2^{(1)}(t_{12})\}$,$s_1^{(1)}(t_{12})$代表为 mp_i 提供虚假资源,$s_2^{(1)}(t_{12})$代表为 mp_i 提供携带病毒的资源.r_i 此时采用$s_1^{(1)}(t_{12})$策略的概率为 x_2,采用 $s_2^{(1)}(t_{12})$策略的概率为 $1-x_2$,$x_2\in[0,1]$.mp_i 的策略集为 $S_2(t_2)=\{s_1^{(2)}(t_2),s_2^{(2)}(t_2)\}$,$s_1^{(2)}(t_2)$代表 mp_i 与 r_i 建立连接,$s_2^{(2)}(t_2)$代表 mp_i 与 r_i 不建立连接.mp_i 此时采用$s_1^{(2)}(t_2)$策略的概率为 y,采用 $s_2^{(2)}(t_2)$策略的概率为 $1-y$,$y\in[0,1]$.

设 mp_i 遇到善意 r_i 的概率为 a,mp_i 遇到恶意 r_i 的概率为 $1-a$.

将 r_i 为善意节点时的期望收益记为 $E_1^G(x_1,y)$,r_i 为恶意节点时的期望收益记为 $E_1^B(x_2,y)$,mp_i 的期望收益记为 $E_2(x_1,x_2,y)$.

$$E_1^G(x_1,y)=x_1y \tag{7}$$

$$E_1^B(x_2,y)=x_2+4y-2x_2y-2 \tag{8}$$

$$E_2(x_1,x_2,y)=(4ax_1-3ax_2+3x_2+5a-6)y-2ax_1+(a-1)x_2-2a+2 \tag{9}$$

由混合策略下的贝叶斯纳什均衡的充要条件,应存在下列不等式组.

$$\begin{aligned}&E_1^G(x_1=0,y)\leqslant E_1^G(x_1,y)\\&E_1^G(x_1=1,y)\leqslant E_1^G(x_1,y)\\&E_1^B(x_2=0,y)\leqslant E_1^B(x_2,y)\\&E_1^B(x_2=1,y)\leqslant E_1^B(x_2,y)\\&E_2(x_1,x_2,y=0)\leqslant E_2(x_1,x_2,y)\\&E_2(x_1,x_2,y=1)\leqslant E_2(x_1,x_2,y)\end{aligned} \tag{10}$$

将 $x_1=0$ 和 $x_1=1$ 分别代入式(7)并化简得到不等式组(11).

$$\begin{cases}x_1y\geqslant 0\\y(1-x_1)\leqslant 0\end{cases} \tag{11}$$

将 $x_2=0$ 和 $x_2=1$ 分别代入式(8)并化简得到不等式组(12).

$$\begin{cases}x_2(1-2y)\geqslant 0\\(1-2y)(x_2-1)\geqslant 0\end{cases} \tag{12}$$

将 $y=0$ 和 $y=1$ 分别代入式(9)并化简得到不等式组(13).

$$\begin{cases}[4ax_1-3x_2(a-1)+5a-6]y\geqslant 0\\[4ax_1-3x_2(a-1)+5a-6](y-1)\geqslant 0\end{cases} \tag{13}$$

采用双矩阵博弈的作图求解方法可得.

当 $a=\frac{1}{2}$时,贝叶斯纳什均衡解的集合为$\{(1,0),(0,1),(1,0)\}\cup\{(1,0),(1,0),(y,1-y)\},y\in[0,1/2]$.

当 $a>\frac{1}{2}$时,贝叶斯纳什均衡解的集合为$\{(1,0),(0,1),(1,0)\}\cup\{(1,0),(\frac{2-3a}{1-a},\frac{2a-1}{1-a}),(1/2,1/2)\}$

当 $a<\frac{1}{2}$时,无贝叶斯纳什均衡解.由以上结论可

以得到定理 3.

定理 3 （mp_i 的节点选择策略）

①当 mp_i 遇到善意 r_i 节点的概率为 1/2 时,存在两种策略.一个是善意 r_i 节点会为 mp_i 提供安全可靠的资源,恶意 r_i 节点会为 mp_i 提供携带病毒的资源,而 mp_i 会建立与 r_i 节点的连接;另一个是善意 r_i 节点会为 mp_i 提供安全可靠的资源,恶意 r_i 节点会为 mp_i 提供虚假资源,而 mp_i 会以概率 y 与 r_i 节点建立连接,以概率 $(1-y)$ 不与 r_i 建立连接,$y\in[0,1/2]$.

②当 mp_i 遇到善意 r_i 节点的概率大于 1/2 时,同样存在两种策略.善意 r_i 节点会为 mp_i 提供安全可靠的资源,恶意 r_i 节点会为 mp_i 提供携带病毒的资源,而 mp_i 会建立与 r_i 节点的连接;另一个是善意的 r_i 节点会为 mp_i 提供安全可靠的资源,恶意的 r_i 节点会以 $\frac{2-3a}{1-a}$ 的概率为 mp_i 提供虚假资源、以 $\frac{2a-1}{1-a}$ 的概率为 mp_i 提供携带病毒的资源,而 mp_i 会以 1/2 的概率与 r_i 节点建立连接,或以 1/2 的概率不与 r_i 建立连接.

③当 mp_i 遇到善意 r_i 节点的概率小于 1/2 时,mp_i 不与 r_i 节点建立连接.

4　DSTM_MP2P 的性能评估

4.1　仿真参数设置

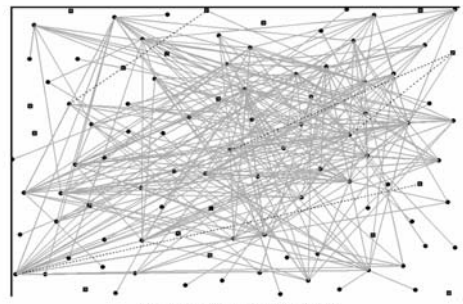
为了评估 DSTM_MP2P 模型的性能,在 J-Sim 仿真平台对模型进行了实现.仿真实验设想的应用场景是 MP2P 文件共享应用.仿真实验参数见表 3.仿真实验的硬件环境为 1.73GHz 双核处理器和 2G 内存.每项仿真均采用执行 10 次后取平均值.

表 3　仿真参数表

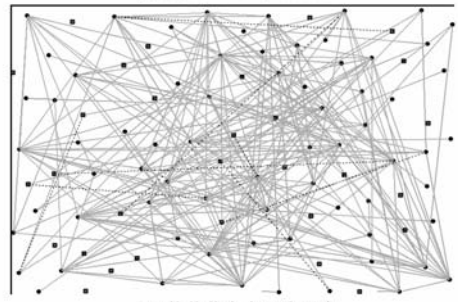
参数	描述	默认值
m	节点总数	100
m/k	每个簇中平均包含节点的个数	10
B_w/Mbps	通信带宽	11
Mobility Model	移动模型	Random Waypoint
Speed/m·s^{-1}	节点移动的速度	1.4
G	网络中善意节点的初始比例	10%
α	网络中历史信息已知的节点比例	30%
β	伪善节点在恶意节点集合中所占的比例	60%
Simulation time/s	仿真时间	3600

4.2　性能评估

以下两幅图为不同条件下,节点依据 DSTM_MP2P 模型进行交互的仿真拓扑关系图.图 1 为网络中恶意节点占 30%,信任历史信息已知的节点占 50% 情况下的拓扑关系,其中图 1(a)表示的是伪善节点表现为善意时的拓扑结构,图 1(b)表示的是伪善节点表现为恶意时的拓扑结构.图 2 为网络中恶意节点占 30%,信任历史信息已知的节点也占 30% 情况下的拓扑结构,图 2(a)和图 2(b)与图 1(a)和图 1(b)表示的含义相同.从图中不难发现,无论网络中善意与恶意节点的比例以及信任历史信息已知节点与未知节点的比例如何变化,请求节点依据 DSTM_MP2P 模型总是优先选择安全可靠的资源节点进行连接.此外,从图中还发现有大量

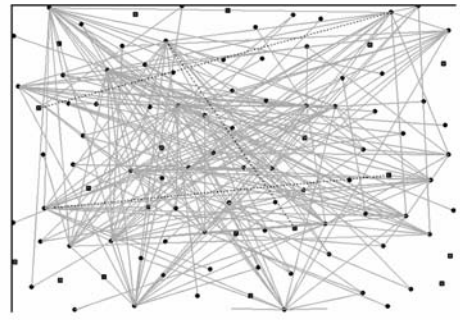


(a) 伪善节点表现为善意

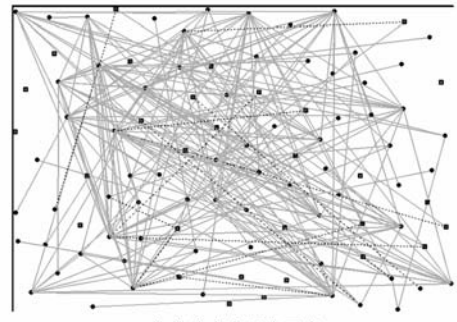


(b) 伪善节点表现为恶意

图1　30%的恶意节点, 50%的节点信息已知



(a) 伪善节点表现为善意



(b) 伪善节点表现为恶意

图2　30%的恶意节点,30%的节点信息已知

的恶意节点与可信的 MP2P 网络分割.这就表明 DSTM_MP2P 无论在如何复杂多变的环境下,总可以以较大的概率判定节点的性质.之后与安全的节点建立一条可信的链路.

下面对 DSTM_MP2P 模型的文件下载成功率进行仿真,结果如图 3 所示.实验模拟了网络中存在 10% 的恶意节点、30% 的恶意节点、50% 的恶意节点和 80% 的恶意节点四种情况下,随着网络中历史信息已知的节点比例变化情况下的下载成功率.

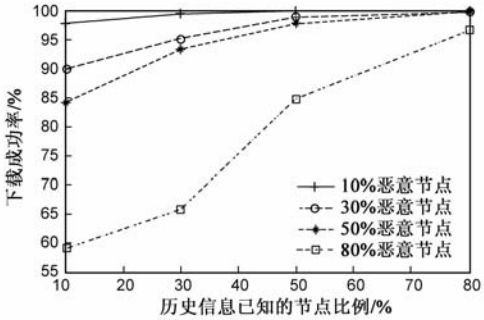


图3 历史信息已知的节点比例变化下的下载成功率

从图中不难发现,随着历史信息已知的节点比例增大,下载成功率逐渐增高,在恶意节点占网络中节点数的 10%、30% 和 50% 时,无论网络中历史信息已知的节点比例如何变化,下载成功率在[85%,100%]区间内变化.在恶意节点占网络中节点数的 80% 时,其下载成功率在[59.4%,96.39%]区间内变化.这主要是由于 DSTM_MP2P 模型在历史信息已知与历史信息未知的情况下采用两套的不同策略所致.从而反向验证了 DSTM_MP2P 模型的有效性.

如图 4 所示为网络中恶意节点比例变化下,NoTrust、GossipTrust 和 DSTM_MP2P 三种模型在 20% 信息未知和 50% 信息未知情况下的下载成功率.从图中不难发现,在 MP2P 网络中不采用信任模型,下载成功率在[9%,42%]区间内变化,显然无法满足用户的需求.对于 P2P 网络中的 GossipTrust 尽管比 NoTrust 的下载成功率高,但也只是在[12%,79%]区间内变化.尤其是当网络中信任历史信息未知的节点比例增加时,其下载成功率急速递减.这主要是 GossipTrust 仅适用于 P2P 网络,而对于 MP2P 网络环境下存在信任历史信息未知的情况没有考虑所导致的.反观 DSTM_MP2P 模型的下载成功率,无论环境如何变化,其下载成功率始终在[84.86,99.81]区间内变化.从而保障网络的服务质量和用户体验.再次从对比角度验证了 DSTM_MP2P 模型的有效性,表明 DSTM_MP2P 模型更适合 MP2P 网络环境.

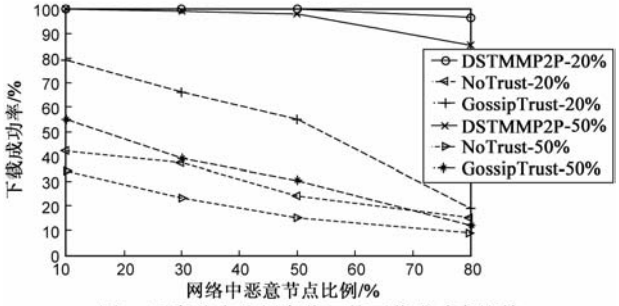


图4 恶意节点比例变化下的下载成功率比较

5 结论

针对 MP2P 网络环境下的信任问题,提出一种 MP2P 网络动态安全信任模型 DSTM_MP2P.本文的主要贡献包括:(1) 针对节点的信任历史信息已知或部分已知的情况,提出基于节点行为函数的节点类型识别机制.(2) 针对节点的信任历史信息未知的情况,提出基于贝叶斯博弈的节点概率选择策略.理论分析和仿真实验结果一致表明,无论环境如何变化,利用 DSTM_MP2P 模型的资源请求节点总是优先连接安全可靠的资源节点,从而极大提高了下载成功率.

参考文献

[1] 李景涛,荆一楠,肖晓春,等.基于相似度加权推荐的 P2P 环境下的信任模型[J].软件学报,2007,18(1):157 – 167.
Li Jing-tao, Jing Yi-nan, Xiao Xiao-chun, et al. A trust model based on similarity-weighted recommendation for P2P environments[J]. Journal of Software, 2007, 18(1): 157 – 167. (in Chinese)

[2] Xiong L, Liu L. Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities[J]. IEEE Transactions on Knowledge and Data Engineering, 2004, 16(7): 843 – 857.

[3] 田春岐,邹仕洪,王文东,等.一种基于推荐证据的有效抗攻击 P2P 网络信任模型[J].计算机学报,2008,31(2):270 – 280.
Tian Chun-qi, Zou Shi-hong, Wang Wen-dong, et al. A new trust model based on recommendation evidence for p2p networks[J]. Chinese Journal of Computers, 2008, 31(2): 270 – 280. (in Chinese)

[4] 胡波,王汝传,王海艳.基于集对分析的 P2P 网络安全中的信誉度改进算法[J].电子学报,2007,35(2):244 – 247.
Hu Bo, Wang Ru-chuan, Wang Hai-yan. A modified security solution based on SPA for servents' reputations in P2P systems [J]. Acta Electronica Sinica, 2007, 35(2): 244 – 247. (in Chinese)

[5] Zhou R, Hwang K, Cai M. Gossiptrust for fast reputation aggregation in peer-to-peer networks [J]. IEEE Transactions on Knowledge and Data Engineering, 2008, 20(9): 1282 – 1295.

[6] Chen K, Hwang K, Chen G. Heuristic discovery of role-based trust chains in peer-to-peer networks[J]. IEEE Transactions on

Parallel and Distributed Systems,2009,20(1):83 – 95.
[7] J Fu,H Xiong,L Zhou,et al. Perform trust:Trust model integrated past and current performance in P2P file sharing systems [A]. Proceedings of the IEEE/ACS International Conference on Computer Systems and Applications[C]. Piscataway:IEEE Press,2008.718 – 725.
[8] Z Yan. A conceptual architecture of a trusted mobile enviroment[A]. Proceedings of the Second International Workshop on Security,Privacy and Trust in Pervasive and Ubiquitous Computing[C]. Piscataway:IEEE Press,2006.75 – 81.
[9] E Palomar,J M E Tapiador,J C H Castro. Dealing with sporadic strangers,or the (un)suitability of trust for mobile P2P security[A]. Proceedings of the 18th International Workshop on Database and Expert Systems Applications[C]. Piscataway:IEEE Press,2007.779 – 783.
[10] W Y Lai,C M Chen,B Jeng. Information exchange mechanism based on reputation in mobile P2P networks[A]. Proceedings of the Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing[C]. Piscataway:IEEE Press,2007.2.643 – 646.

作者简介

李致远　男,1981 年生于河南开封,在读博士生,主要研究方向为 P2P 网络安全,无线传感器网络.
E-mail:lizhiyuan81@126.com

王汝传　男,1943 年生于安徽合肥,教授,博士生导师,主要研究方向为计算机软件,计算机网络和网格,对等计算,信息安全,无线传感器网络等.
E-mail:wangrc@njupt.edu.cn